PTA / PIA: FDA - GIMS - QTR3 - 2025 - FDA4950158

Created Date: 8/13/2025 8:54 PM Last Updated: 9/9/2025 4:25 PM

General Information

PTA / PIA Name:	FDA - GIMS - QTR3 - 2025 - FDA4950158	**PTA / PIA ID:**	3645591
Component Name:	FDA - HFP Genomic Information Management System	**ATO Boundary Name:**	HFP Amazon Web Services East Applications
Overall Status:	Complete	**# of Days - Open:**	27
Submitter:		**Submit Date:**	9/3/2025
Next Assessment Date:	N/A	**Expiration Date:**	1/1/2100
Office:		**OpDiv:**	FDA
Security Categorization:	Low		
Make PIA available to Public?:	Yes	**PIA Required:**	Yes

General 01:	Identify the Enterprise Performance Lifecycle Phase of the system.	Operations and Maintenance
General 02:	Is this a FISMA-Reportable system?	No
General 03:	Does the system have or is it covered by a Security Authorization to Operate (ATO)?	No
General 04:	ATO Date or Planned ATO Date.	7/3/2025
General 05:	Is the system or electronic information collection, agency or contractor operated?	Agency
History Log:	View History Log	

Privacy Threshold Analysis

Privacy Threshold Analysis

PTA 01:	Point of Contact (POC) Name	Sabina Lindley
PTA 01A:	POC Title and Organization	Project Manager, HFP
PTA 01B:	POC Email Address	Sabina.Lindley@fda.hhs.gov
PTA 01C:	POC Phone Number	240-402-2959
PTA 02:	Indicate the following reason(s) for this PTA. Choose from the following options.	PIA Validation (PIA Refresh)
PTA 02A:	Describe in further detail any changes to the system that have occurred since the last PIA.	No changes
PTA 03:	Is the data contained in the system owned by the agency or contractor?	Agency
PTA 04:	Please give a brief overview of the purpose of the system by describing what the functions of the system are and how the system carries out those functions in support of HHS.	GIMS serves as HFP's central repository and tracking system for pathogen genomic surveillance data. It provides HFP microbiology laboratories with a centralized, integrated system for managing genomic data from foodborne pathogens. Functioning as both a database and an analysis platform, GIMS automates data retrieval from sequencing instruments across HFP laboratories, executes routine analyses using the high-performance computing (HPC) cluster, and facilitates data submission to the National Center for Biotechnology Information (NCBI). Additionally, it supports data imports from external laboratories via Illumina's BaseSpace.
PTA 05:	List and/or describe all the types of information that are collected, maintained, and/or shared by the system regardless of whether that information is PII and how long that information is stored.	The only PII in the system is the username and password of system users.
PTA 05A:	Are user credentials used to access the system?	Yes, but the user credentials are maintained in a separate system (e.g., AD, AMS) and not collected or maintained by this system.
PTA 05C:	Please identify the system that maintains the user credentials or controls access to this system.	AD for LDAP accounts, local database for accounts that are not PIV exempt
PTA 06:	Describe why each type of information is collected, maintained, and/or shared by the system. Specify what information is collected about each category of individual.	The only PII in the system is the username and password of system users. This information is used to establish a user role in GIMS and to restrict access to the GIMS application by non-authorized FDA employees and direct contractors.
PTA 07:	Does the system collect, maintain, use, or share PII?	Yes
PTA 08:	Does the system include a website or online application?	No
PTA 14:	Does the system have a mobile application?	No
PTA 20:	Are any third-party websites or applications (TPWA) associated with the system?	No
PTA 21:	Does this system use artificial intelligence (AI) tools or technologies?	No

Privacy Impact Assessment

Privacy Impact Assessment

PIA 22:	Indicate the type(s) of personally identifiable information (PII) that the system will collect, maintain, or share.	Biographical Information User Credentials
PIA 23:	Indicate the categories of individuals about whom PII is collected, maintained, or shared.	Employees/HHS Direct Contractors
PIA 24:	Indicate the approximate number of individuals whose PII is maintained in the system.	<100
PIA 25:	For what primary purpose is the PII used?	The username and password is used to establish a user role in GIMS and to restrict access to the GIMS application by non-authorized FDA employees and direct contractors.
PIA 26:	Describe any secondary uses for which the PII will be used (e.g., testing, training, or research).	The FDA makes no secondary use of the PII.
PIA 28:	Identify legal authorities, governing information use and disclosure specific to the system and program.	The implementation of this system is authorized by 5 U.S.C. 301 which permits agency heads to create the usual and expected infrastructure necessary for the organization to accomplish its purposes and mission. In addition, the security and privacy measures of the system are required by the Federal Information Security Management Act (FISMA) and the statutes underlying OMB Circular A-130 for the secure and efficient use of government systems and resources.
PIA 29:	Are records in the system retrieved by one or more PII data elements?	No
PIA 30:	Identify the sources of PII in the system.	Government Sources Within the OPDIV
PIA 31:	Is there an Office of Management and Budget (OMB) information collection approval number?	No
PIA 31B:	Explain why an OMB information collection approval number is not required.	The Paperwork Reduction Act (PRA) is N/A, only collecting username and password.
PIA 32:	Is the PII in the system shared directly with other organizations outside the system's Operating Division?	No
PIA 33:	Is the submission of PII by individuals voluntary or mandatory as defined in the Privacy Act?	Voluntary

PIA 34:	Describe the method in place to notify and obtain consent from individuals whose PII will be collected. If no prior notice is given or consent cannot be obtained, explain why.	Submission of PII is voluntary as that term is used by the Privacy Act. There is no opt-out opportunity or method. Administrators necessarily control and manage the creation of user credentials, the only PII in GIMS. Users who independently change their password must submit it to GIMS in order for the Agency to process administrative materials and securely administer access to Agency information and property. Permanent employees, direct contract employees, fellows and other personnel voluntarily provide their PII that is handled in the separate Active Directory system used by GIMS Administrators when generating user credentials. Notice and opt-out mechanisms associated with Active Directory are outside the scope of this GIMS assessment.
PIA 35:	Describe the process to notify and obtain consent from the individuals whose PII is in the system when major changes occur to the system (e.g., disclosure and/or data uses have changed since the notice at the time of original collection). If they cannot be notified or have their consent obtained, explain why.	Submission is voluntary.
PIA 36:	Describe the process in place to resolve an individual's concerns when they believe their PII has been inappropriately obtained, used, or disclosed, or that the PII is inaccurate. If no process exists, explain why not.	Individuals who suspect their PII has been inappropriately obtained, used or disclosed in any FDA system have a number of avenues available to request to rectify the situation. Often, these individuals contact the office or division where they have determined that their information is held. Individuals may then make further requests for their information to be corrected or amended. FDA considers these requests and, if appropriate, makes the requested changes. Employees with such concerns can additionally work with their supervisor, a 24-hour technical assistance line, FDA's Systems Management Center, and other channels.
PIA 37:	Describe the process in place for periodic reviews of the system to ensure the integrity, availability, accuracy, and relevancy of the PII in the system. Please address each element in your response. If no processes are in place, explain why not.	FDA Personnel are responsible for providing accurate information and may independently update and correct their information at any time.
PIA 38:	Identify who will have access to the PII in the system.	Users Administrators Contractors
PIA 38A:	Select the type of contractor.	HHS/OpDiv Direct Contractors
PIA 38B:	Do contracts include Federal Acquisition Regulation (FAR) and other appropriate clauses ensuring adherence to privacy provisions and practices?	Yes

PIA 39:	Provide the reason why each of the groups identified in 38 needs access to PII.	Users will not have access to others' logon credentials. Users will only be allowed to change their own passwords. GIMS Administrators are responsible for creating and maintaining user accounts, but they will not have access to users passwords. User passwords are self created for each account. If an Administrator needs to reset a password, a temporary password is sent in which the user is able to use to change their password. Some users will also be FDA direct contractors
PIA 40:	Describe the administrative procedures in place to determine which system users (administrators, developers, contractors, etc.) may access PII.	Management establishes the roles for individual personnel accessing GIMS on a case-by-case basis and the only PII in the system are user access credentials. Program management determines which users, direct contractors, and administrators are granted access to the GIMS systems on a case-by-case basis. Although administrators may have access to usernames in the course of creating and maintaining accounts, they will not have access to user passwords.
PIA 41:	Describe the technical methods in place to allow those with access to PII to access only the minimum amount of information necessary to perform their job.	Roles for individual personnel are established, with role-based restrictions permitting access only to information that is required for each individual to perform his/her job.
PIA 42:	Identify the general security and privacy awareness training provided to system users (system owners, managers, operators, contractors and/or program managers) to make them aware of their responsibilities for protecting the information being collected and maintained.	The FDA requires all Agency personnel to complete FDA's IT Security and Privacy Awareness training at least once every 12 months. A portion of this training is dedicated to guidance on recognizing and safeguarding PII.
PIA 43:	Describe the training system users receive above and beyond general security and privacy awareness training.	Additional on-the-job or informal training may be received.
PIA 44:	Describe the process and guidelines in place for the retention and destruction of PII. Cite specific National Archives and Records Administration (NARA) records retention schedule(s) and include the retention period(s).	Retention is maintained under FDA File Code 9962 and National Archives and Records Administration (NARA) General Records Schedule (GRS) 20, Item 1c; superseded by the new GRS 3.2, item 030 (DAA-GRS-2013-0006-0003), which is for “records … created as part of the user identification and authorization process to gain access to systems. Records are used to monitor inappropriate systems access by users. This schedule applies to records such as “user profiles; log-in files; password files; audit trail files and extracts; system usage files; and cost-back files used to assess charges for system use.” Under this schedule, retention is until "when business use ceases." In other words, NARA concurs that agencies may dispose of these records as soon as they are no longer needed.

PIA 45:	Describe how the PII will be secured in the system using administrative, technical, and physical controls. Please address each element in your response.	Administrative safeguards include user training; system documentation that advises on proper use; implementation of Need to Know and Minimum Necessary principles when awarding access, and others. Technical Safeguards include network monitoring, two-factor authentication for network access, and password for system access. Physical controls include that all system servers are located at FDA facilities protected by guards, locked facility doors, and climate controls. Other appropriate controls have been selected from the National Institute of Standards and Technology's (NIST's) Special Publication 800-53, as determined using Federal Information Processing Standard (FIPS) 199.

Review and Comments

OpDiv Privacy Analyst Review

Privacy Analyst Review Decision:	Approved	**Privacy Analyst Review Date:**	9/3/2025
Privacy Analyst Review Comments:		**# of Days - PA Review:**	0

SOP Review

SOP Review Decision:	Approved	**SOP Review Date:**	9/3/2025
SOP Review Comments:		**# of Days - SOP Review:**	0

Agency Privacy Analyst Review

Agency Privacy Analyst Review Decision:	Approved	**Agency Privacy Analyst Review Date:**	9/4/2025
Agency Privacy Analyst Review Comments:	Reviewer: Crystal Bland 9/4/2025 All comments have been addressed. 9/2/2025 Please see comment and update accordingly. PTA-5: Per PTA-6, please include in your response "The only PII in the system is the username and password of system users."	**# of Days - APA Review:**	1

SAOP Review

SAOP Review Decision:	Approved	**SAOP Review Date:**	9/9/2025
SAOP Review Comments:		**# of Days - SAOP Review:**	5

SAOP Signature

Date	User	Type	Name	Original Value	New Value
9/9/2025 3:04 PM	BAUR, VANESSA	Signature	SAOP (Email PIN)		Content Signed

Supporting Document(s)

Name	Size	Type	Upload Date	Downloads
No Records Found				

Comments

Question Name	Submitter	Date	Comment	Attachment
PTA 01	BLAND, CRYSTAL	8/19/2025	8-19-2025 Per FDA's Email (unable to attached email and exported PIA), The PIA is experiencing an Archer error with Question #3 of the general information (Q-3 “Does the system have or is it covered by a Security Authorization to Operate (ATO)?” The FDA instance of Archer is automatically entering the answer “No,” which is incorrect. **The ATO date is 7/3/2025.** At this time, we are unable to update Archer to reflect the correct answer “Yes.”	
PTA 05	BLAND, CRYSTAL	9/2/2025	Per PTA-6, please include in your response "The only PII in the system is the username and password of system users."	